806 KAR 3:230. Standards for safeguarding customer information.

RELATES TO: KRS 304.99-020, 15 U.S.C. 6801, 6805(b), 6807
STATUTORY AUTHORITY: KRS 304.2-110(1), 15 U.S.C. 6801(b)
NECESSITY, FUNCTION, AND CONFORMITY: KRS 304.2-110(1) authorizes the executive director to promulgate reasonable administrative regulations necessary for or as an aid to the effectuation of any provision of the Kentucky Insurance Code, as defined in KRS 304.010. The Gramm-Leach-Bliley Act as codified in 15 U.S.C. 6801(b) requires the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of these records; and (3) to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer. This administrative regulation establishes the appropriate standards for licensees of the Office of Insurance to safeguard customer information. The Gramm-Leach-Bliley Act extends particularly to financial institutions, however, this administrative regulation applies to all licensees of the office regardless of whether or not the licensee is considered a financial institution for purposes of the Gramm-Leach-Bliley Act.

Section 1. Definitions. (1) "Consumer" means an individual who seeks to obtain, obtains, or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family, or household purposes, and about whom the licensee has nonpublic personal information; or that individual’s legal representative.

(2) "Customer" means a consumer who has a customer relationship with a licensee.

(3) "Customer information" means nonpublic personal information about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

(4) "Customer information systems" means the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

(5) "Customer relationship" means a continuing relationship between a consumer and a licensee under which the licensee provides one (1) or more insurance products or services to the consumer that are to be used primarily for personal, family, or household purposes.

(6) "Licensee" means all insurers holding a certificate of authority, licensed producers, companies, or business entities licensed or required to be licensed, or authorized or required to be authorized, or registered, excluding service contract makers, or required to be registered pursuant to the Kentucky Insurance Code as defined in KRS 304.1-010.

(7) "Service provider" means a person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

Section 2. Information Security Program. Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Section 3. Objectives of Information Security Program. A licensee's information security program shall be designed to:

(1) Ensure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information; and

(3) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Section 4. Determined Violation. A violation of this administrative regulation may constitute an unfair trade practice in the business of insurance and shall subject the licensee to a civil penalty authorized by KRS 304.99-020.

Section 5. Effective Date. Each licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to Sections 1 to 3 of this administrative regulation, within 180 days of the effective date of this administrative regulation.

Section 6. Incorporated by Reference. (1) SAFE-1, "Examples of Methods of Development and Implementation (August 2003 Ed)" is incorporated by reference.

(2) This material may be inspected, copied, or obtained, subject to applicable copyright law, at the Office of Insurance, 215 West Main Street, P.O. Box 517, Frankfort, Kentucky 40602, Monday through Friday, 8 a.m. to 4:30 p.m. This material is also available at http://doi.ppr.ky.gov/kentucky/. (30 Ky.R. 774; Am. 1308; 1517; eff. 1-5-2004; TAm eff. 8-9-2007.)